IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

SNNO: 2347–3657
Volume 9,Issue1 Feb ,2021

Modern Secure Cloud Architecture

Mr. Pulime Satyanarayana[1] , Mrs. A. Rajini Devi[2], Mr. Vemula Pranay[3]

Abstract: *Cloud security architecture may be a security strategy designed around securing an organization's data and applications within the cloud. it's a critical extension of enterprise security, and it requires an architecture to attach it with an overall security approach. In cloud security architecture, responsibility is shred between the cloud provider and customer. As more organizations sift and share their data within the cloud, the more important it becomes to possess a security architecture in situ to secure data. The cloud are often delivered in multiple formats. As such, cloud security architectures are designed to figure during a combination of software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) environments -- additionally to areas like the general public or private cloud. During this paper we identify the foremost vulnerable security threats/attacks in cloud computing, which can enable both end users and vendors to understand about the key security threats related to cloud computing and propose relevant solution directives to strengthen security within the Cloud environment. We also propose secure cloud architecture for organizations to strengthen the safety.*

Keywords: Cloud Computing, Security, Secure Cloud Architecture, Security and Privacy

INTRODUCTION

[1] Cloud computing is that the delivery computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the web ("the cloud") to supply faster innovation, flexible resources, and economies of scale. you sometimes pay just for cloud services you employ , helping lower your operating costs, run your infrastructure more efficiently and scale as your business needs change.

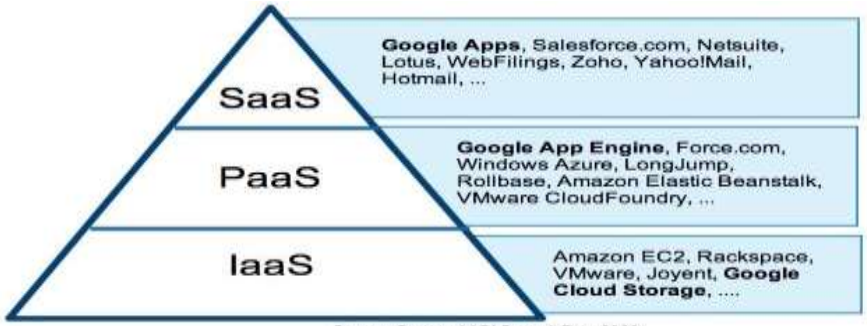
With Cloud Computing becoming a well-liked term on the knowledge Technology (IT) market, security and accountability has become important issues to spotlight . There are variety of security issues/concerns related to cloud computing but these issues fall under two broad categories: Security issues faced by cloud providers and security issues faced by their customers.

Department of Computer Science Engineering, Samskruti College of Engineering and Technology

SNNO: 2347–3657
Volume 9,Issue1 Feb ,2021

International Journal of
Information Technology & Computer Engineering

Most cloud computing services fall under four broad categories: infrastructure as a service (IaaS), platform as a service (PaaS), serverless and software as a service (SaaS). These are sometimes called the cloud computing stack because they repose on top of 1 another. Knowing what they're and the way they're different makes it easier to accomplish your business goals. [2] A picturing of the cloud modal is shown below by Gartner



Source: Gartner AADI Summit Dec 2009

1.1 Infrastructure as a Service (IaaS)

The most basic category of cloud computing services. With IaaS, you rent IT infrastructure-servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis.

1.2 Platform as a Service (PaaS)

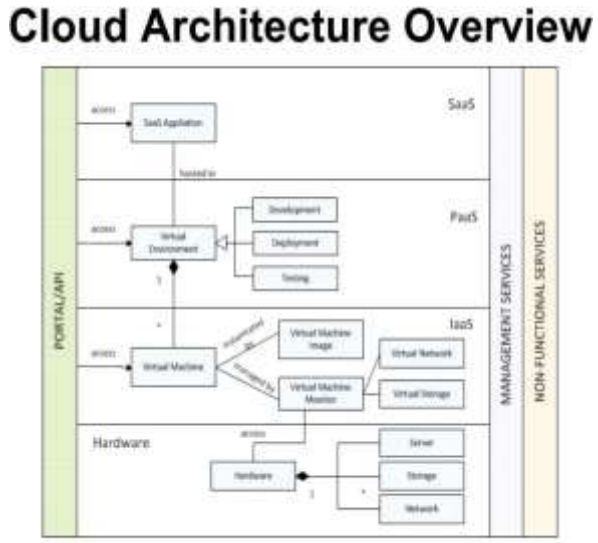
Platform as a service refers to cloud computing services that provide an on-demand environment for developing, testing, delivering and managing software applications. PaaS is meant to form it easier for developers to quickly create web or mobile apps, without fear about fixing or managing the underlying infrastructure of servers, storage, network and databases needed for development.

1.3 Software as a Service (SaaS)

Software as a service my be a method for delivering software applications over the web , on demand and typically on a subscription basis. With SaaS, cloud providers host and mange the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users hook up with the appliance over the web, usually with an internet browser on their phone, tablet or PC.

1.4 Serverless Computing

Overlapping with PaaS, serverless computing focuses on building app functionality without spending time continually managing the servers and infrastructure required to try to so. The cloud provider handles the setup, capacity planning and server management for you. Serverless architectures are highly scalable and event-driven, only using resources when a selected function or trigger occurs.



Cloud Architecture Overview

I. RELATED WORK

[3] Our approach allows to separate the underlying computations into their security and performance aspects: the security-critical operations are performed by the Trusted Cloud in a Setup Phase, whereas the performance critical operations are performed on encrypted data by the Commodity Cloud. This allows maximum utilization of the expensive resources of

SNNO: 2347–3657
Volume 9,Issue1 Feb ,2021

the Trusted Cloud, while high loads of queries can be processed on-demand by the Commodity Cloud. The Trusted Cloud requires only a constant amount of storage and is used constantly in the Setup Phase for pre- computing encryptions. The untrusted Commodity Cloud provides a large amount of storage.

[5] Data classification is the process that allows organizations and individuals to categorize all different kinds of data and information assets according to its confidentiality degree, which will determine the extent of security the data needs. Classification is made to guarantee information sensitivity and an appropriate protection for the by-low protected information. Data can also be categorized in accordance to how frequently it must be accessed i.e. t its critical value. Data with higher critical value will be stored on a faster media whereas data that are less critical are stored on slower media. Different encryption algorithms and cryptographic functions such as Secure Hashing Algorithm (SHA)16, Advanced Encryption Standard (AES)17 and Transport Layer Security (TLS)19 are used based on the security level of the data

[6] investigated the problem of assuring the customer of the integrity (i.e.correctness) of his data in the cloud. The cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised since the data is physically not accessible to the user. The authors provided a scheme which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the cloud provider and the customer and can be incorporated in the service level agreement. The authors suggested that this scheme ensures that the storage at the client side is minimal which will be beneficial for thin clients.

[7] the authors analyzed vulnerabilities and security risks specific to cloud computing systems. They defined four indicators for cloud-specific vulnerability including: 1) it is intrinsic to or prevalent in core technology of cloud computing, 2) it has its root in one of NIST's essential cloud characteristics, 3) it is caused by cloud innovations making security controls hard to implement, 4) it is prevalent in established state-of-the- art cloud offerings. The authors were certain that additional cloud-specific vulnerabilities will be identified; others will become less of an issue as the field of cloud computing matures. However, they believe that using a precise definition of what constitutes vulnerability and the four indicators they identified will provide a level of precision and clarity that the current discourse about cloud computing security often lacks.

In [8] the authors proposed an Effective Privacy Protection Scheme (EPPS) to provide the appropriate privacy protection for cloud services. EPPS satisfies users' privacy requirements and maintains system performance simultaneously. First, they analyzed the privacy level users require and quantified the security degree and performance of encryption algorithms. Then, an appropriate security composition is derived by the results of analysis and quantified data. Their simulation results showed that the EPPS not only fulfils users' privacy requirements but also maintains the cloud system performance in different cloud environments.

[9] Security and privacy requirements: identifies security and privacy requirements for the cloud such as authentication,authorization, integrity, etc. Attacks and threats: warns from different types of attacks and threats to which clouds are vulnerable. Concerns and risks: pay attention to risks and concerns about cloud computing. We discuss each guideline in detail in the following sub-sections.

SNNO: 2347–3657
Volume 9,Issue1 Feb ,2021

International Journal of
Information Technology & Computer Engineering

II. THREATS TO CLOUD COMPUTING

The most common forms of threat concerned with cloud are as follows:

A. Crytojacking

[11] Crytojacking may be a fairly new sort of cyber attack, and it's also one which will very easily go under the radar. It centers round the popular practice of mining for cryptocurrencies like Bitcoin.

[12] Cryptojacking may be a sort of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or maybe servers) by cyber criminals to mine for cryptocurrency. Like many sorts of cybercrime, the move is profit, but unlike other threats, it's deigned to remain completely hidden from the victim. Cyber criminals hack into devices to put in cryptojacking software. The software works within the background, mining for cryptocurrencies or stealing from cryptocurrency wallets. The unuspecting victims use their devices typically, though they'll notice slower performance or lags. In early 2018, the CoinHive miner was fund to be running on YouTube Ads through Google's DoubleClick platform.

B. Data Breaches

Perhaps the for most common threat to cloud computing is that the issue of leaks or loss of knowledge through data breaches. a knowledge breach typically occurs when a business is attacked by cybercriminals who are ready to gain unauthorized access to the cloud network or utilize programs to look at , copy, and transmit data.

If you employ cloud computing services, a knowledge breach are often extremely damaging, but it can happen relatively easily. Losing data can violate the overall Data Protection Regulation (GDPR), which could cause your business to face heavy fines.

C. Denial of Service

One of the foremost damaging threats to cloud computing may be a denial of service (DoS) attack. These can pack up your cloud services and make them unavailable both to your users and customers, but also to your staff and business as

an entire. There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives an excessive amount of traffic for the server to buffer, causing them to hamper and eventually stop. Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is shipped that takes advantage of bugs within the target that subsequently crash or severely destabilize the system, in order that it can’t be accessed or used.

D. Insider Threats

When we consider cyber security challenges, we frequently consider the concept of malicious criminals hacking into our systems and stealing data

International Journal of
Information Technology & Computer Engineering

SNNO: 2347–3657
Volume 9,Issue1 Feb ,2021

– however, sometimes the matter originates from the within of the corporate . In fact, recent statistics suggest that insider attacks could account for quite 43 percent of all data breaches.

Insider threats are often malicious – like members of staff going rogue – but they will even be thanks to negligence or simple human error. it's important, then, to supply your staff with training, and also make sure that you're tracking the behavior of employees to make sure that they can't commit crimes against the business.

E. Hijacking Accounts

Perhaps the best threat to a business that uses cloud computing technologies is that the challenge of hijacked accounts. If a criminal can gain access to you system through a staff account, they might potentially have full access to all or any of the knowledge on your servers without you even realizing any crime has taken place. Cybercriminals use technique like password cracking and phishing emails so as to realize access to accounts – so once more , the key here is to supply your team with the training to know the way to minimize the danger of their account being hijacked.

F. Insecure Applications

Sometimes it are often the case that your own system is very secure, but you're disappointed by external applications. Third-party services, like applications, can present serious cloud security risks, and you ought to make sure that your team or cyber-security experts take the time to determine whether the appliance is suitable for your network before tey need it installed. Discourage staff from taking matters into their own hands and downloading any application that they think could be useful. Instead, you ought to make it necessary for the IT team to approve any application before it's installed on the system. While this might sound sort of a lengthy step to place in situ , it can effectively deduct the danger of insecure applications.

Installing third party modules often results in security aspects not being checked rigorously and trusting the appliance to be secure. Hence it's necessary to a certain the documentation of the module and use the simplest practices in integrating it into your applications.

G. Inadequate Training

Most cyber security threats are available the shape of outsider attacks, but this issue is one caused by a drag inside thecorporate . And this problem is in failing to require the threat of cybercrime seriously. it's essential to take a position intraining on the risks of cyber attacks – not only for your IT team, except for every member of staff. Your team is yourfirst line of defense against any quite data breach or cyber attack, in order that they got to be prepared with the newestinformation or relevant threats to businesses like yours. Allocate time and allo staff training, and also confirm that this training is often updated in order that your staff is being taught about issues that are genuinely affecting organizations. A good training session could also be lengthy but is extremely necessary for all of the people using the appliance toknow how it works and what shouldn't be done which will compromise the safety of the appliance .

III. TYPES OF ATTACKS ON CLOUD COMPUTING

4.1 Cloud Malware Injection Attacks

[13] the foremost common sorts of malware injection attacks are cross-site scripting attacks and SQL injection attacks.During a cross-site scripting attack, hackers add malicious scripts (Flash, JavaScript, etc.) to a vulnerable website .

German researchers arranged an XSS attack against the Amazon Web Services cloud computing platform in 2011.within the case of SQL injection, attackers target SQL servers with vulnerable database applications. In2008,Sony's PlayStation website became the victim of a SQL injection attack.

Attack mitigation: it's necessary to implement Content Security Policy (CSP)to scale back the severity of the attck, should also implement appropriate Headers within the response from the server.

4.2 Abuse of Cloud Services

Hackers can use cheap cloud services to rearrange DoS and brute force attacks on track users, companies, and even other cloud providers. as an example , security experts Bryan and Anderson arranged a DoS attack by exploiting capacities of Amazons EC2 cloud infrastructure in 2010.As a

SNNO: 2347–3657
Volume 9,Issue1 Feb ,2021

result, they managed to form their client unavailable on the web by spending only to rent virtual services.
Attack mitigation: To implement a check on the amount of requests coming from an endpoint and to limit it after exceeding the utmost request count. Enterprises must monitor those that have access to the cloud and found out mitigations for any threats or risks.

4.3 Denial of Service Attacks

DoS attacks are designed to overload a system and make services unavailable to its users. These attacks are especially dangerous for cloud computing systems, as many users may suffer because the results of flooding even one cloud server. just in case of high workload, cloud systems begin to supply more computational power by involving more virtual machines and repair instances. While trying to stop a cyber attack, the cloud system actually makes it more devastating. Finally, the cloud system slows down and bonafide users lose any availability to access their cloud services. within the cloud environment, DDoS attacks could also be even more dangerous if hackers use more zombie machines to attack an outsized number of systems.
Attack mitigation: Enterprises must monitor those that have access to the cloud and found out mitigations for any threats or risks. The always-on option is enabled through DNS redirection. It stops application layer assaults attempting to determine TCP connections with an application in an attempt to exhaust server resources.

4.4 Side Channel Attacks

A side channel attack is arranged by hackers once they place a malicious virtual machine on an equivalent host because the target virtual machine during a side channel attack, hackers target system implementations of cryptographicalgorithms.
Attack Mitigation: However, this sort of threat are often avoided with a secure system design. [14] Eliminating cache information leakage, Introducing "random noise" into the computation, Using tamper resistance and hostile environment detection.

4.5 Wrapping Attacks

A wrapping attack is an example of man-in-the-middle attack within the cloud environment. Cloud computing issusceptible to wrapping attacks because cloud users typically hook up with services via an internet browser. An XMLsignature is employed to guard users' credentials from unauthorized access, but this signature doesn't secure thepositions within the document. Thus, XML signature element wrapping allows attackers to contro an XML document. For example, a vulnerability was found within the SOAP interface of Amazon Elastic Cloud Computing (EC2) in 2009.This weakness allowed attackers to switch an eavesdroppd message as a results of a successful signature wrappingattack.
Attack Mitigation: [15] We proposed FastXPath to point to the signed subtree, and showed that it's fulfilling this taskduring secure and performant way, disabling signature wrapping attacks for all reasonable scenarios.

4.6. Man-in-the-Cloud Attacks

During this sort of attack, hackers intercept and reconfigure cloud services by exploiting vulnerabilities within the synchronization token system in order that during subsequent synchronization with the cloud, the synchronization tokenare going to be replaced with a replacement one that gives access to the attackers. Users may never know that their accounts are hacked, as an attacker can replace the first synchronization tokens at any time. Moreover, there's a risk that compromised accounts will never be recovered.
Attack Mitigation: Use a VPN, be careful for phishing scams.

4.7. Insider Attacks

An insider attack is initiated by a legitimate user who is purposefully violating the safety policy. During a cloud environment, an attacker are often a cloud provider administrator or an employee of a client company with extensive privileges.
Attack Mitigation: to stop malicious activity of this sort, cloud developers should design secure architectures with different levels of access to cloud services.
The other solution to the present problem is to stay a track of all the members actively involved the appliance development and maintenance. Also proper training for the appliance should tend before the utilization of it.

4.8 Account or service hijacking

Account or service hijacking is achieved after gaining access to a user's credentials. There are

International Journal of
Information Technology & Computer Engineering

SNNO: 2347–3657
Volume 9,Issue1 Feb ,2021

various techniques for achieving this, from fishing to spyware to cookie poisoning. Once a cloud account has been hacked, attackers can obtain a user's personal information or corporate data and compromise cloud computing services. as an exmple , an employee of Sales force, a SaaS vendor, became the victim of a phishing scam which led to the exposure of all of the company's client accounts in 2007.

Attack Mitigation: Install Firewalls Around Your DNS Resolver, Increase Restrictions on Access to call Servers, Prevent Cache Poisoning.

4.9. New Attacks: Spectre and Meltdown

These two sorts of cyber attacks appeared earlier this year and have already become a replacement threat to cloud computing. With the assistance of malicious JavaScript code, adversaries can read encrypted data from memory by exploiting design weakness in latest processors. Both Spectre and Meltdown break the isolation between applications and therefore the OS , letting attackers read information from the kernel. this is often a true headache for cloud developers, as not all cloud users install the newest security patches

Attack Mitigation: [16] As a playful counterpoint to Intel's CAT system, the researchers dubbed their method "DAWG", which stands for "Dynamically Allocated Way Guard." (The dynamic part means DAWG can split the cache into multiple buckets whose size can vary over time.)

IV. SECURE CLOUD ARCHITECTURE

5.1 Implement RBAC Pattern

Simple yet effective, when implemented properly will keep out unauthorised access to cloud services.

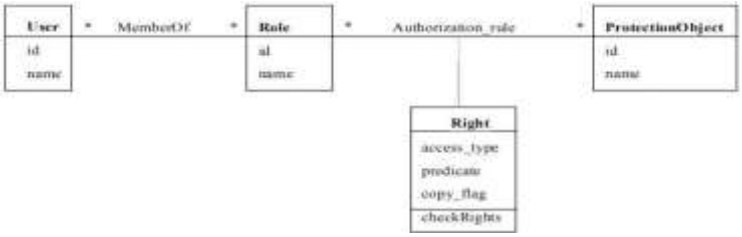


Figure: Basic RBAC Pattern

Users are assigned roles consistent with their functions and given the needed rights (access types for specific objects).When users are assigned by administrators, this is often a compulsory model. Can implement least privilege and separation of duty policies.

5.2 Single Check In (SSO)

[18] Single sign-on (SSO) is an authentication scheme that permits a user to log in with one ID and password to any of sever alerted, yet independent, software systems. True single sign-on allows the user to log in once and access services without re-entering authentication factors. an easy version of single sign-on are often achieved over IP networks using cookies but as long as the sites share a standard DNS parent domain.

5.3 Network Segmentation

Network segmentation may be a useful gizmo to form sure your data isn't [19] an excellent majority of servers or hosts in these centers are going to be found to be virtualized hosts (having the server virtualization product – the hypervisor running inside them) for reasons of scalability, agility, cost-efficiency of operations and maybe even security.

The VXLAN based network segmentation are often configured to supply isolation among resources of multiple tenants of a clud data center as follows. a specific tenant are often assigned two or more VXLAN segments (or IDs). The tenant can utilize he multiple VXLAN segments for assigning them to different tiers (Web, Application or Database) of the appliance the tenant is hosting within the data center. Selective connectivity are often established among VXLAN segments belonging to an equivalent tenant while communication between VXLAN segments belonging to different ten ants are often prohibited.

With the increasing adoption of cloud services by large enterprises that need to host multi-tier applications, the info center network administrators

SNNO: 2347–3657
Volume 9,Issue1 Feb ,2021

need a versatile virtual networking topology with capability to get the specified isolation through network segmentation. At an equivalent time, it's necessary that these virtual network segments span mutiple, arbitrary IP subnets of the info center and also several hypervisor clusters. As of now, the sole virtual networking technology which will provide these capabilities without an excellent deal of physical network reconfiguration or addition of networking resources is that the overlay-based virtual networking.

5.4 Intrusion Detection System and Intrusion Prevention System (IDS/IPS)

[20] **Behaviour-based IDS:** Statistical Anomaly Detection (or behaviour-based detection) may be a methodology where statistical techniques are wont to detect penetrations and attacks these begin by establishing base-line statistical behaviour: what's normal for this system? They then gather new statistical data and measure the deviation from the base-line. If a threshold is exceeded, issue an alarm.

Knowledge-based IDS: Most commercial IDS search for attack signatures: specific patterns of network traffic or activity in log files that indicate suspicious behaviour are referred to as knowledge-based or misuse detection IDS.

Host based IDS: Derived from mere log file analysers modern host based Intrusion Detection Systems are designed as host based applications running within the background of presumed critical, sensitive hosts, like Mail Servers, DNS Servers, web servers, database servers, etc. Especially in e-commerce environments, where sensitive data are stored or availability is critical, host based IDS are found predominantly.

Network based IDS A network-based IDS monitors network traffic on packet level. The components are the network based IDS software, running on a fanatical host, connected to the network traffic with a network interface, and again an IDS management station, where the software is run and alerts are sent to.

IPS: An IPS are often defined as an in-line product that focuses on identifying and blocking malicious network activity in real time. generally , there are two categories: rate-based products; and content-based (also mentioned as signture and anomaly-based). The devices often appear as if firewalls and sometimes have some basic firewall functionality. But firewalls block all traffic except that that they need a reason to pass, whereas IPS pass all traffic except that that they need a reason to dam .

5.5 Virtual firewalls

[21] A virtual firewall then may be a firewall service or appliance running entirely within a virtualised environment — whilst another virtual machine, but even as readily within the hypervisor itself — providing the standard packet filtering and monitoring that a physical firewall provides. The VF are often installed as a standard software firewall on a guest VM already running within the virtualized environment; or it are often a purpose-built virtual security appliance designed with virtual network security in mind; or it are often a virtual switch with additional security capabilities; or it are often a managed kernel process running within the host hypervisor that sits atop all VM activity.

The current direction in virtual firewall technology may be a combination of security-capable virtual switches, and virtual security appliances. Some virtual firewalls integrate additional networking functions like site-to-site and remote access VPN, QoS, URL filtering and more.

5.6 Deep Protection

Deep Protection refers to the concept of implementing protection not just to urge into the system but to also add an additional layer of protection while completing some critical actions inside the system. an honest thanks to apply this is often to feature during a confirmation password entry or a confirmation panel asking the user to validate the action before performing a critical action.

5.7 SaaS Level Protection

A Cloud service provider often features a set of excellent security measures and features already implemented consistent with the industry standard. So it's important to examine the service they're providing and using it to the simplest of our advantage.

[22] Cloud Access Secrity Brokers (CASB) offers logging, auditing, access control and encryption capabilities whichwill be critical when investigating security issues during a SaaS product.

Some security measures which will be implemented which are readily available by top level cloud service

SNNO: 2347–3657
Volume 9,Issue1 Feb ,2021

providers:Logging and alerting
IP white lists and/or blacklists
API gateway, if the servicer often accessed using APIs

5.8. Proper Cloud Storage Configuration

Cloud storage configuration is one of the crucial parts of setting up a secure cloud architecture. Setting up proper access control rights for all the logins and to divide up and assigning proper security groups should be done carefully. Controlling who has the right to do what on the cloud will help us to know the origin of the problem if any occurs. An example of this can be amazons AWS 'I AM ROLE' configurations.

5.9 Setting up Data Loss Prevention Tools

Backing up your data o regular basis and setting up proper DLP (Data loss prevention) tools will help in prevention of unauthorised movement of intellectual property stored on the cloud.

5.10 Offline Backups

It may seem to much of a sep to take but backing up yur most crucial data offline will help you in times when a cloud is compromised, like in ransomeware, where you are locked out and don't have the option of accessing the cloud.

V. CONCLUSION

In conclusion it is safe to say that cloud computing is still in its infant stages. But with strict rules and appropriate measures we can make cloud computing a lot secure. Cloud architecture should implement tried and tested security measures which have been in the market for a long time. Implementing security measures such as SSO(Single Sign on), RABC pattern, Network segmentation, IDS / IPS, Virtual Firewalls, Deep Protection and SaaS level protection we can

protect cloud from a lot of security threats. Cloud Computing has the potential to have a great impact on the world. It has many benefits that it provides thereto users and businesses. For example, some of the benefits that it provides to businesses, is that it reduces operating cost by spending less on maintenance and software upgrades and focus more on the businesses itself. But there are other challenges the cloud computing must overcome. People are very typical about whether their data is secure and personal . There are no standards or regulations worldwide provided data through cloud computing. Europe has data protection laws but the US, being one among the foremost technological advance nation, doesn't have any data protection laws. Users also worry about who can disclose their data and have ownership of their data. But once, there are standards and regulation worldwide, cloud computing will revolutionize the future.

ACKNOWLEDGMENT

I would like to acknowledge the University of Mumbai, Mumbai, India to give me the opportunity to do the research work under the title “Secure Cloud Architecture in Modern Age”. I would like to acknowledge the college L.B.H.S.S Trust’s Institute of Computer Application, Mumbai, India to support during the research process.

REFERENCES

[1]. https://searchcloudsecurity.techtarget.com/definition/cloud-security-architecture [Tom Nolle]

[2]. https://download.huihoo.com/google/gdgdevkit/DVD1/developers.google.com/appengine/training/intro/whatiscc/index.html [Gartner]

[3]. Twin Clouds: An Architecture for Secure Cloud Computing, Sven Bugiel1, Stefan N¨urnberger1, Ahmad-Reza Sadeghi1, Thomas Schneider2 https://cachin.com/cc/csc2011/submissions/bugiel.pdf

[4]. Secure Cloud Architecture, Kashif Munir1and Prof Dr. Sellapan Palaniappan2 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1084.

[5]. A Secure Cloud Computing Model based on Data Classification, Lo’ai Tawalbeh1,* , Nour S. Darwazeh2, Raad S. Al-Qassas2 and Fahd AlDosari1 https://www.sciencedirect.com/science/article/pii/S1877050915009503

[6]. R. Sravan Kumar and A. Saxena, “Data

SNNO: 2347–3657
Volume 9,Issue1 Feb ,2021

integrity proofs in cloud storage", Third International Conference on Communication Systems and Networks (COMSNETS), 2011.

[7]. Vadym Mukhin, Artem Volokyta, "Security Risk Analysis for Cloud Computing Systems" The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Prague, Czech Republic, 15-17 September 2011

[8]. I. Chuang, S. Li, K. Huang, and Y. Kuo, "An effective privacy protection scheme for cloud computing", In Proceeding of the 13th International Conference on Advanced Communication Technology (ICACT), 2011

[9]. A Framework for A Framework for Framework forSecure Cloud ure Cloudure Cloud ure CloudComputing,

Ahmed E. Youssef1 and Manal Alageel2, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.401.9191 **[10].** https://www.researchgate.net/figure/Seven-Threats-in-Cloud-computing-1_fig1_327173990

[11]. https://cloudacademy.com/blog/key-cybersecurity-threats-to-cloud-computing/

[12]. https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking

[13]. https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks

[14]. https://www.intertrust.com/blog/side-channel-attacks-strategies-and-defenses/

[15]. Analysis of Signature Wrapping Attacks and Countermeasures, Sebastian Gajek, Meiko Jensen, Lijun Liao,and Jorg Schwenk https://lists.w3.org/Archives/Public/public-xmlsec/2009Nov/att-0019/Camera-Ready.pdf

[16]. https://news.mit.edu/2018/mit-csail-dawg-better-security-against-spectre-meltdown-attacks-1018

[17]. https://owasp.org/www-pdf-archive/SecResearchOWASP7-2013.pdf

[18]. https://en.wikipedia.org/wiki/Single_sign-on

[19]. Analysis of Network Segmentation Techniques in Cloud Data Centers, Ramaswamy Chandramouli https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=918440

[20]. Intrusion Detection Systems and Intrusion

[21]. Prevention Systems, Andreas Fuchsberger, https://faculty.kfupm.edu.sa/ics/salah/092/ics444/slides/IDS%20and%20IPS.pdf

[22]. https://en.wikipedia.org/wiki/Virtual_firewall

[23]. https://cloud.netapp.com/blog/blg-cloud-security-architecture-for-iaas-paas-and-saas